AN ENDNOTE ON REGULATING CYBERSPACE: ARCHITECTURE VS LAW?

GRAHAM GREENLEAF*

I. INTRODUCTION: KING CANUTE'S COMEBACK

About a millennium ago, King Canute became known for issuing executive orders (perhaps because of a lack of time for formal legislation) against forces of nature: to wit, to turn back the waves. His lack of success is notorious.[1]

With such a start, you might reasonably expect this article to proceed to the usual warnings about the futility of governments trying to regulate the unstoppable forces of cyberspace.[2] In fact, my drift will be largely in the opposite direction: regulation of the 'nature' of cyberspace – 'architecture' as it is called later on – may often be the most effective form of regulation, and may sometimes be necessary to preserve important values. We need some King Canutes in cyberspace.[3]

There is relatively little writing about a general theoretical structure for the regulation of cyberspace. Such a theoretical structure is needed to enable us to assess whether current or proposed laws (or the absence of them) are the best or only regulatory options available. This article comments on some of the forms that such a theoretical approach might take and gives examples of its application, including some drawn from Australian law.

Much of this article discusses how governments could legislate to affect or

* BA LLB (Syd) MACS; Professor of Law, University of New South Wales.

1 Sveynsson, Canute II the Great (995-1035), King of England and Denmark has had a bad press. However, he was probably being ironic if "According to Legend, he proved to flatterers the limits of his powers by demonstrating his inability to induce the waves to recede": *Directory of Royal Genealogical Data*, University of Hull at: <http://www.dcs.hull.ac.uk/cgi-bin/gedlkup/n=royal?royal01548>.

2 For example John Perry Barlow, who compared the US Government's attempts to stop the use of strong encryption via the 'Clipper Chip' with 'the folly of King Canute': see JP Barlow, "Jackboots on the Infobahn" *Wired* 2.04 at <http://www.hotwired.com/Lib/Privacy/privacy.barlow.html>; or P Waters and L Carver who say that "the Internet is as inevitable and overwhelming as the incoming tide which confronted King Canute, and renders the traditional approach of regulation and prohibition futile": P Waters and L Carver "The Internet and Telephony: The Impact of Uncontrollable Technology on Traditional Telephony Regulation" Gilbert and Tobin website at <http://www.gtlaw.com.au/gt/bin/frameup.cgi/gt/pubs/telephony.html>.

3 These sovereigns will act without irony, their laws will be effective. However, the effectiveness of laws regulating architecture will not necessarily serve benign ends, as is discussed later.

control cyberspace architecture in various situations, and the effects that this might have, but the purpose is not to argue for governments to regulate architecture more extensively. Rather, the aim is to illustrate that architecture is not neutral but embodies choices and values: it reflects the interests of the 'codewriters',[4] and its legitimacy as regulation can and should sometimes be questioned on this basis.

I start by discussing how our views of the nature of cyberspace have changed over the last few years, then outline where we might start to develop a comprehensive approach to assessing regulatory options in cyberspace, and conclude with examples of how it can shed light on current and proposed instances of cyberspace regulation.

II. THE EVOLVING NATURE OF CYBERSPACE

A. A Realm of Freedom? The Myths of Digital Libertarianism

Much of the earliest and most influential writing about cyberspace was from a decidedly libertarian perspective, written by people excited by the early pre-commercial Internet's potential to create virtual communities and customs which seemed to have little relation to the nation state or the practices of 'real space'.[5] James Boyle has described this approach as,[6]

> it was not so much that nation states would not want to regulate the Net, it was that they would be unable to do so, forestalled by the *technology of the medium*, the *geographical distribution of its users*, and the *nature of its content*. This tripartite immunity came to be a kind of Internet Holy Trinity, faith in which was a condition of acceptance into the community.

To Boyle's Trinity of famous sayings I have added two more myths of digital libertarianism.[7] A quick comment on each will indicate why cyberspace is developing in a contrary direction. Detailed discussion of some of these examples will be saved until later in the paper.

(i) "On the Internet, no one knows you're a dog" (New Yorker cartoon)[8]

This famous cartoon encapsulated the belief that cyberspace was a realm of anonymity and pseudonymity, where you could browse the web in privacy, or adopt a pseudonym (and new sex or history if you like) for interactions with others. In fact, it is increasingly closer to the truth to say that the default condition of our interactions and communications in real space is anonymity, whereas the

---

4 L Lessig's terminology, discussed later.

5 Or 'meat space' as John Perry Barlow called it.

6 J Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty and Hard-Wired Censors" (1997, draft only): original available at <http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm>); copy available at <http://www2.austlii.edu.au/itlaw/secure/foucault.htm>.

7 The first and last in the following five.

8 'There's a now classic joke about cyberspace that first appeared as a cartoon in the New Yorker magazine: A dog and cat are sitting in front of a computer. Former says to the latter, "On the Internet, no one knows you're a dog" quoted at <http://www.umass.edu/pubaffs/online/archives/96/041596.html>.

default condition of Internet communications is some form of identification,[9] and many businesses and governments are investing in increasing the level of identification.

(ii) "Information wants to be free" (Stewart Brand)[10]

The process of digitisation of works made them infinitely reproducible at virtually no marginal costs, and infinitely distributable via the Internet. The Internet and property in information were widely believed to be incompatible, and technology would win against law and set information free. The reverse process is now underway: technical protections of intellectual property over networks may protect property interests in digital artefacts more comprehensively than has ever been possible in real space, and destroy the public interest elements in intellectual property law in the process. In the worst scenarios, the surveillance mechanisms being developed to do this may also bring about the end of the anonymity of reading. Perhaps the true version of Brand's aphorism will turn out to be "Information wants to be free ... but it wants to keep *you* under surveillance".

(iii) "The Net interprets censorship as damage and routes around it" (John Gilmore)[11]

The Internet's structural resistance to censorship is supported by well-publicised cases of data being moved from one server to the next to continue its availability, and by the numerous routes that can be found to any page on the web by those savvy enough to wish to avoid attempts at censorship. It is also an accurate reflection of the Internet's technical origins, it having been designed to re-route messages around outages caused by nuclear war. However, this resistance to censorship is easily over rated, and the structure of cyberspace may in fact facilitate pervasive censorship (at least for the majority of non-savvy users). There are a number of reasons for this. Technologies such as PICS (Platform for Internet Content Selection) were ostensibly developed to facilitate individual and parental (rather than state) choice and control of 'content selection' through third party content filters. But there is nothing in the technology to stop the content selection (and thus the choice of third party filter) being imposed at a level higher up network hierarchies than that of the individual user.[12] The use of content filters by

---

9 As yet, it is usually only something weaker than true identification, such as unauthenticated pseudonymity, since machine addresses and even email addresses are not unambiguous or non-repudiable: see G Greenleaf "Privacy principles: Irrelevant to Cyberspace?" (1996) 3 *Privacy Law & Policy Reporter* 114. However, others such as Jerry Kang see the same default condition emerging: 'in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase": J Kang, "Cyberspace Privacy: A Proposal Regarding the Private Sector's Processing of Personal Information Generated in Cyberspace" (1998) *Stanford Law Review* (forthcoming), cited in Lawrence Lessig "The Architecture of Privacy" (Draft 2), *Taiwan Net '98*, Taipei March 1998: <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf>.

10 Almost always attributed (without any source) to Stewart Brand, EFF board member, founder of Whole Earth Catalog and the WELL. One list of famous quotes adds "Among others. No telling who really said this first.": <http://world.std.com/~tob/quotes.htm>.

11 That Gilmore, a founder of the Electronic Frontier Foundation, did say this is well attested, but the exact occasion is obscure: see Boyle, note 6 *supra* at <http://www2.austlii.edu.au/itlaw/secure/foucault.htm#N_4_>

12 See Boyle note 6 supra, part III for a brief discussion.

employers, universities and even the state (where international Internet connectivity is through a very limited number of channels) may make Internet censorship pervasive, and sometimes remote. Second, the Internet's potential for surveillance of our browsing habits encourages the self-censorship of the panopticon.

(iv) "In Cyberspace, the First Amendment is a local ordinance" (John Perry Barlow)[13]

Barlow's ironic[14] comment was a reminder that cyberspace can be resistant to regulation by any particular local sovereign. Information that the government of Burma may wish to suppress may be untouchable on a server in the USA. Activities such as Internet gambling (and its profits) may be run from a server on some tropical island. There are a number of reasons why the limits of national sovereigns to control the Internet are exaggerated, but the principal one is that nations are increasingly acting in concert to deal with the borderless nature of cyberspace by creating both relatively uniform laws across jurisdictions (for example, the WIPO Copyright Convention and the European Union's privacy Directive), and agreements for international cooperation in surveillance and investigation (for example, the Wassenar Agreement concerning encryption export controls). There is also the fact that those who wish to evade national laws mainly operate at the margins: there are problems in running significant commercial organisations from underdeveloped countries, and in spending the profits thus generated. While not disregarding the Internet as a source of regulatory arbitrage[15], location matters for reasons other than the regulatory climate.

(v) "A Declaration of the Independence of Cyberspace" (John Perry Barlow[16] again)

In Barlow's 1996 'Declaration' he asserted that "[y]our legal concepts of property, expression, identity, movement, and context do not apply to us", and generally gave a pugnacious assertion of the 'keep your hands off our Internet' approach, directed against the nation states and governments of the world. The demand for independence even finds echoes in the judgment of Dalziel J in the original judgment striking down the USA's *Communications Decency Act*[17] as unconstitutional: "As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion".[18]

Boyle's critique of digital libertarianism, and particularly its claim to the

---

13 JP Barlow "Leaving the Physical World" presented at Conference on HyperNetworking, Oita, Japan: <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html>.

14 The intended irony in Barlow's comment is that the First Amendment protects freedom of communication via Internet in the USA, rather than restricts it, so it is not only prohibitions that have the limitations of locality.

15 cf M Froomkin, "The Internet As A Source of Regulatory Arbitrage" in B Kahin and C Nesson (eds), *Borders in Cyberspace*, MIT Press (1997).

16 <http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration>.

17 *Communications Decency Act* of 1996, Pub L No 104-104, tit V, 1996 USCCAN (110 Stat) 56, 133; available at <http://www.cdt.org/policy/freespeech/12_21.cda.html>.

18 *American Civil Liberties Union v Reno*, 929 F Supp 824 (ED Pa 1996); available at: <http://www.ciec.org/decision_PA/decision_text.html>.

'independence' of cyberspace, is based on both "its blindness towards the effects of private power, and the less familiar claim that digital libertarianism is also surprisingly blind toward the state's own power in cyberspace".[19] The technological solutions to legal problems preferred by the 'digiterati' (such as PICS and P3P) are not as neutral or benign as they are believed to be, he argues. The paradox is that to 'protect mass speech' and to protect other values, the Internet may sometimes need 'government intrusion', as the rest of this article explores.

Barlow's 'Declaration' may seem like the last gasp of digital libertarianism, but we now hear distorted echoes of this approach in the insistence by some governments that, at least whenever consumer interests such as privacy are involved, voluntary self-regulation by Internet businesses can be trusted to produce an answer.

B. A Realm of Surveillance? A Dystopian View of Cyberspace

In contrast with the digital libertarians is a view of cyberspace which emphasises the likely extent of identification and surveillance in cyberspace, and its potential for misuse. A version of this argument is sketched below.[20] At this stage of the Internet's development, my view is that the jury is still out, and whether the repressive or the liberating potential of the Internet prevails (or some mix of both) depends on political decisions and technical developments yet to occur.

(i) The Pervasiveness of Cyberspace

The twenty first century will see life teeming in cyberspace. Irrespective of their level of computer literacy, education, interest or consent, everyone in at least the advanced industrial economies will spend a significant portion of time 'in' cyberspace by the early years of the twenty first century. People may not always realise that what they are doing is 'on the Internet', but the reality appears from a few simple factors. Transactions with business and government will much more commonly take place via information systems that are connected to the Internet. Many tools that people use in their work, such as inventory control systems, medical diagnostic equipment, will be connected to the Internet as a means of distributing data to remote parts of an organisation. These tools will tend to require information about who their user is, for security and accountability purposes. We will communicate with others in various public, semi-public and private ways via cyberspace, and obtain some portion of our entertainment from it.

(ii) Surveillance by Default

One consequence of our living a large part of our lives in cyberspace is simply that, whether we know or care, large quantities of personal information about each of us will be collected via a pervasive, worldwide-network (and stored on

19 Boyle, note 6 *supra*, "Introduction".

20 An earlier version of this section appeared in G Greenleaf, "Privacy and cyberspace: An ambiguous relationship" (1996) 3 *Privacy Law & Policy Reporter* 88.

machines connected to it). This is an event new in world history. The accessibility or interconnectedness of this information is contingent on several factors, including custom, public opinion and law, but is unlikely to be contingent on any serious technical considerations. Because the information will have been collected by processes related to one pervasive network, any impediments to its being found, published, or related to other data elsewhere on the Internet are easily removed if those who control the information wish to remove them. The great protectors of privacy of the past such as cost, distance, incompatibility and undiscoverability , are all disappearing in the face of the Internet and its protocols - the great equalisers of the twenty first century.

Cyberspace interactions are prima facie not anonymous, because we disclose potentially identifying (or interaction-enabling) information[21] such as name, email address or machine address in the act of communicating, unless we make a conscious effort not to do so. Widespread use of digital signatures will make them more strongly identified. In real space the default state of communications has been that they are anonymous unless we choose to identify ourselves or are already known to the other party.

(iii) Identity and Digital Personae

So we will all have a digital persona, which Roger Clarke describes as "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual",[22] a representation in cyberspace of who and what we are. A digital persona may be active or passive.[23] In fact, we will have multiple digital personae, as each organisation with which we deal will do so on the basis of different data about us available to it. We need to distinguish between those parts of a person's digital personae which are in 'public' spaces in the sense of being able to be found by Internet search engines or other means, and those parts which are in non-public spaces, either 'proprietary' (the databases of a government or company) or 'personal' (information found only on the networked computers of the person the subject of the information, or those that person has provided it to, such as by email). Those who hold parts of our digital personae in proprietary (or 'closed') systems can easily cumulate that information with our total 'public' digital persona, as well as combining it with that held in other proprietary systems to which they have access. From the cumulative effect of our digital personae, others will draw inferences about our personalities and behaviour. The extent to which we will be able (technically and/or legally) to exercise some control over what makes up our digital personae will be an important issue. Whether the use of anonymous or pseudonymous transactions

---

21 As in note 9 *supra*, this is as yet usually only something weaker than true identification. The use of digital signatures, discussed below, may change this.

22 R Clarke, "The Digital Persona and its Application to Data Surveillance" (1994) *The Information Society* March 1994; for abstract only: <http://www.anu.edu.au/people/Roger.Clarke/DV/AbstractDigPersona.html>.

23 Clarke makes a useful distinction between the "passive digital persona", the cumulation of details of our transactions and communications that are discoverable on the Internet (our snail tracks), and the 'active digital persona', the computerised 'agents' of various types that actively affect what information the user receives or discloses (ranging from filters rejecting or classifying or replying to incoming mail, to 'knowbots' regularly trawling for information that the user wants).

will be prohibited, or in some cases will be required, is discussed in the later example 'Building anonymity into architecture'.

(iv) Identification at the Cyberspace / Real Space Interface

We only exist virtually in cyberspace: the digital persona is only a representation of the physical person that exists in real space. Identification occurs at the cyberspace/real space interface. In cyberspace it has often been relatively easy to impersonate someone. Recognising individuals over distance and time without recourse to human memory has always been a key organisational challenge to bureaucracies.[24] Tokens, knowledge and biometrics, or combinations of these, provide the links between the physical person and the file. Identification in cyberspace intensifies the challenge because it removes any physical settings or proximity which assist identification, and it often requires real time responses. The reliability of electronic commerce, or email and other Internet transactions, or the believability of a person's digital persona, depends to a very large extent on the continuing reliability of links between the virtual and physical person.

Biometric identifiers entered directly into networked devices will in the longer run provide a main means of identification. In the more immediate future, smart cards are likely to provide one of the main bridges between physical and virtual identity. They have many potential advantages because they can include in the one token (i) digital representations of value (e-cash or credit); (ii) digital signatures (to provide authentication of messages transmitted); and (iii) digital biometric identifiers (to guarantee security/access to networks). Their portability means they can be the link between mobile people and pervasive networks.

(v) An Encrypted Space: Public Key Infrastructure

Public key (asymmetric) cryptography may be one of the most significant inventions of the twentieth century, information technology's equivalent of the invention of nuclear weapons. A large part of the existence of many people and organisations in cyberspace will be an encrypted one, in that they will be acting via messages and transactions which are encrypted for reasons of confidentiality or authentication or both. Cryptography is likely to be essential for many aspects of the Internet's commercial operations: digital cash; credit transactions; non-repudiation of contracts; authenticity of electronically filed and retrieved documents. Most encrypted transactions will depend upon an infrastructure involving new types of entities such as Certification Authorities. While digital libertarians hailed the potential of encryption to increase privacy of communications, the counterpoint is that the other main use of public key cryptography, authentication through the use of digital signatures, is likely to increase dramatically the extent of strong identification of communications in cyberspace. As with the Internet generally, whether public key cryptography has a repressive or the liberating effect is yet to be determined.

---

24 R Clarke "Human Identification in Information Systems: Management Challenges and Public Policy Issues" (1994) 7 *Information Technology and People* 6: <http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html>.

III. THEORIES OF CYBERSPACE REGULATION DIGITAL REALISM NEEDED

Cyberspace does have characteristics that distinguish it from real space, and they make it more difficult for us to develop a coherent approach to how it should (or should not) be regulated by law. A theory of regulation which is capable of taking account of these unique characteristics is needed, and authors such as a Reidenberg, Boyle, Johnson and Post, and Lessig have put forward candidates.

Joel Reidenberg argues that 'the set of rules for information flows imposed by technology and communication networks form a "Lex Informatica" that policy makers must understand, consciously recognise and encourage'.[25] He argues that the 'technological architectures' of networks impose a set of 'rules for the access to and use of information' distinct from law, and that policy choices are available through control of the technology itself, 'through laws that cause technology to exclude possible options, or through laws that cause users to restrict certain actions'. Reidenberg's work contains many valuable examples of the interplay between 'technological architectures' and law as sources of regulation of cyberspace, but does not provide a sufficiently general approach to determining the most effective way of regulating cyberspace in a particular instance (for example, the roles that morality and markets might play), or a political basis for criticising regulatory options.

Johnson and Post argue[26] for what they call 'net federalism' or 'decentralised, emergent law'. Their argument is that the model for the governance of the Internet which is most likely to be successful is 'de facto rules [which] may emerge as a result of the complex interplay of individual decisions' by various types of system administrators and by users. They argue[27] that:

> Net federalism looks very different than what we have become accustomed to, because here individual network systems, rather than territorially-based sovereigns, are the essential governance units. The law of the net has emerged, and we believe can continue to emerge, from the voluntary adherence of large numbers of network administrators to basic rules of law (and dispute resolution systems to adjudicate the inevitable inter-network disputes), with individual users 'voting with their electrons' to join the particular systems they find most congenial.

Johnson and Post's argument is essentially moral and political, rather than a method of analysis of cyberspace regulation: the architecture of the Internet facilitates a form of self-regulation through a 'collective conversation'; we have not yet tried sufficiently to utilise this capacity; but if we do it will produce the

---

25 J Reidenberg, "Lex Informatica" (1998) 76 *Texas Law Review* 553; see also J Reidenberg, "Governing Networks and Rule-Making in Cyberspace" (1996) 45 *Emory Law Journal* 912-30.

26 DR Johnson and D Post "And How Shall the Net be Governed? - A Meditation on the Relative Virtues of Decentralized, Emergent Law": <http://www.cli.org/emdraft.html>; DR Johnson and D Post "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 *Stanford Law Review* 1367; version available at: <http://www.cli.org/X0025_LBFIN.html>; other papers by Johnson and Post are available at the Cyberspace Law Institute site: <http://www.cli.org/>.

27 'Conclusion, David R Johnson & David Post "And How Shall the Net be Governed? - A Meditation on the Relative Virtues of Decentralized, Emergent Law": <http://www.cli.org/emdraft.html>.

most effective form of regulation.[28]

A more comprehensive theoretical approach to cyberspace regulation is advanced by Lawrence Lessig in a number of articles.[29] To summarise, his starting point is that behaviour is regulated by four types of constraints: laws, social norms, markets and 'nature' (or the 'architecture' of real space). However, this 'anti-law' starting point is counterbalanced by emphasis on the extent to which the law indirectly seeks to regulate behaviour by directly influencing the three other constraints: social norms, markets and (sometimes) 'nature'. Applying this analysis to cyberspace, Lessig identifies the equivalent of 'nature' as 'code, or the software that makes cyberspace as it is, ... a set of constraints on how one can behave', and concludes that code is in general more pervasive and effective ('immediate') a constraint in cyberspace than is nature in real space. However, code is also more susceptible to being changed by law (more plastic) than is nature. Therefore, both code and law (in its indirect form) are more important as regulation of cyberspace than many realise or admit. Also, in order to analyse comprehensively the options available to affect particular behaviours, all four types of constraints (and the potential of law to indirectly regulate via the other three) must be considered.

Lessig describes this approach[30] as part of a more general reaction against the University of Chicago Law School's obsession with the limits of law as a regulator. The 'old' Chicago School's anti-law analysis emphasised the effectiveness (in contrast with law) of both markets and social norms as regulators of individual behaviour, and how both markets and norms were relatively impervious to control by law. A third influential anti-law stream arises from Michel Foucault's work,[31] where the fine-grained controls of continuous surveillance through the 'architectures' of social life (including the built environment, and the social institutions that inhabit it) contrast with the coarse controls of law. In summary, these anti-law approaches emphasise the effectiveness of the three other types of constraint – markets, norms, and 'nature'/'architecture' – at the expense of law.

---

28 'We've hardly tried a collective conversation designed to allow responsible participants to set their own rules and to help all concerned - online and off - seek to understand and respect others' vital interests. Yet that kind of conversation is precisely the kind of activity the net itself is designed - thanks to the engineers - to facilitate': *ibid.*

29 Particularly "The Law Of The Horse: What Cyberlaw Might Teach", 11 June 1998 draft available at: <http://cyber.law.harvard.edu/works/lessig/law_horse.pdf> and via the *Stanford Technology Law Review Working Papers* 1997 draft <http://stlr.stanford.edu/STLR/Working_Papers/97_Lessig_1/index.htm>); see also "Constitution and Code" (1996-7) 27 *Cumberland Law Review* 1; "Intellectual Property and Code" (1996) 11 *St John's Journal of Legal Commentary* Issue 3; "Reading the Constitution in Cyberspace" (1997) 45 *Emory L. J.* 869-910: available at <http://www.law.emory.edu/ELJ/volumes/sum96/lessig.html>; "The Architecture of Privacy" (2nd Draft), *Taiwan Net '98*, Taipei March 1998, available at: <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf> (visited 15/10/08); Lawrence Lessig and Paul Resnick, "The Architectures of Mandated Access Controls": available at <http://cyber.law.harvard.edu/works/lessig/Tprc98_d.pdf>; see also other papers listed at the Harvard site: <http://cyber.law.harvard.edu/lessigcurres.html>.

30 L Lessig, *ibid* in Part 1 "The Regulation of Real Space'.

31 Particularly M Foucault *Discipline and Punish: The Birth of the Prison*, Peregrine Books (1977) (translated by A Sheridan); see also Boyle, note 6 *supra*, at Part 6 "Foucault & the Jurisprudence of Digital Libertarianism"

Digital libertarianism's arguments, that law is destined to be ineffective in cyberspace - are often a particular application of 'anti-law' arguments to the new frontier of cyberspace, which to a large extent borrows from the earlier anti-law streams. The optimistic versions stress the potential for forms of self-regulation in cyberspace, which is to a large extent an emphasis on social norms as regulation. The pessimistic versions are resigned to a world of uncontrollable surveillance and manipulation driven by market imperatives. Both versions see little positive role for law in cyberspace regulation, and that is where Lessig (and Boyle) are correct in differing from them. A theory that recognises and explains the ability of law to regulate cyberspace both for good and for ill could be called 'digital realism', to contrast with both the extremes of optimism and pessimism that a failure to understand the role of law in cyberspace can lead to.

All of the authors mentioned share an emphasis on the importance of the technical infrastructure of cyberspace – whether they call it 'code' or 'Lex Informatica' or 'Net federalism' – as a source of regulation of cyberspace. In my view Lessig presents the most useful and comprehensive theoretical framework, but as I will explain below it is one which needs significant modification, and leads me to prefer the term 'architecture' to 'code'. The rest of this article supports the view that to understand the control (de facto and de jure) of cyberspace architecture is the key to understanding the regulation of cyberspace.

IV. CYBERSPACE REGULATION AS A FUNCTION OF FOUR CONSTRAINTS

A good starting point is to consider in more detail the four types of constraint discussed by Lessig,[32] and the operation of each in cyberspace.

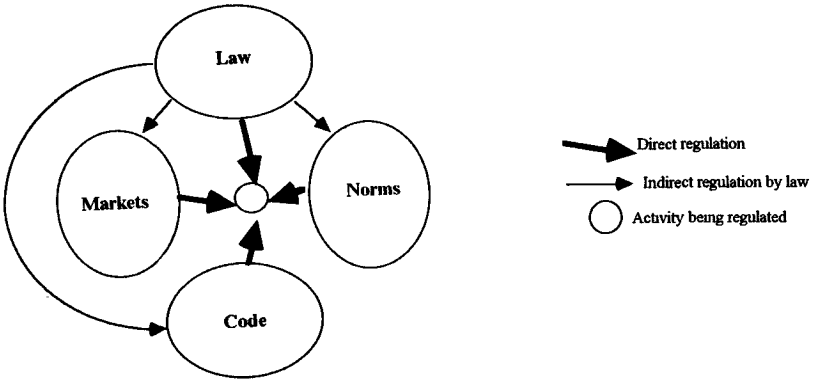

Figure 1: Regulation as a function of four types of constraints (adapted from L Lessig)[33]

32 The section derives from the discussion of the four constraints in L Lessig, note 29 *supra*. The examples used are mine except where noted.

33 Figure 1 is a recreation, not as well drawn and with slightly different headings, of L Lessig's diagram in L Lessig, note 29 *supra*.

A. Norms, Morality and Self-Regulation

In real space social norms cause us to frown on racist jokes or sexist language, to tell the truth about our age where concessions might be available, and to observe other conventions both because we have been brought up to feel guilty if we act otherwise, and also because we fear social embarrassment by doing otherwise (at least if caught). Norms also aid the observance of the sanctions of law by making us guilty about breaking laws even if the likelihood of enforcement is next to nil.

In cyberspace norms play similar roles, and some special ones. The observance of the customs of netiquette by individual Internet users means that you avoid responding to email IN FULL CAPITALS even if you are annoyed (just as you don't shout in arguments), and most people don't send 1 MB attachments to discussion lists with thousands of members. If some Internet businesses voluntarily adopt and adhere to self-regulatory schemes such as the Platform for Privacy Preferences (P3P), then their observance would be because they had adopted the norms of P3P (whatever their motivation for so doing). There is also code/architecture which facilitates P3P, but it does not enforce its norms, as discussed later.

The reasons why norms are effective sanctions in cyberspace are however, likely to be significantly difference from real space. Cyberspace 'morality' may become like the morality of the panopticon or the goldfish bowl. The obvious lesson from Foucault[34] is that, to the extent that we fear and assume surveillance of our activities by others in cyberspace (whether in real time or ex post facto), we are likely to condition our actions to adhere to norms relevant to that behaviour, irrespective of the existence of legal sanctions. For example, anyone visiting websites containing pornographic material will do so conscious that their machine address (at least) will be known to wherever they visit, and potentially traceable back to them. The extent of the fear will often be proportional to their proximity to those likely to be carrying out the surveillance. Surveillance of email by employers is a powerful sanction, as is sharing a computer with a spouse. However, cyberspace tends to obliterate such distances even where they seem to exist. The fear of obviously well-targeted email appearing in your local (under surveillance) email inbox generated by unwise visits to websites on the other side of the world is likely to dissuade some people from such visits.[35]

---

34 M Foucault note 31 supra.

35 In fact this will not usually happen unless you have set your browser software to disclose your email address, or unless your machine address is correlated with your email address on some external source. However, many Internet users will not be sophisticated enough to realise this, and that is the point: the fear of inadvertent disclosure is enough to condition behaviour.

B. Markets

Markets constrain behaviours in obvious ways in real space, influenced by property, contract and other laws which regulate those markets. The market constraints in cyberspace are as important as in real space. Unpopular code/architecture can perish where market forces operate. One distinctive feature of their operation in cyberspace is likely to be network effects, described by Lemley and McGowan as "markets in which the value that consumers place on a good increases as others use the good".[36] Many aspects of the Internet are 'archetypal examples of network markets' in □that they 'involve products whose entire value lies in facilitating access between a consumer and others who own the product'. 'The principal characteristics distinguishing such products ... are the absence of material inherent value and the necessity for common standards among goods incorporated into the network'.[37] Market constraints are not the focus of this article, and will be referred to only incidentally in the examples that follow.

C. 'Code', 'Nature' and 'Architecture'

In real space laws criminalising bank robbery are very helpful, but thick walls, bulletproof glass, armed guards and combination locks on safes are the most effective constraints. We don't need a law on larceny of real property. When considering the combination of constraints which make up regulation in real space, it is easy to ignore the roles of the natural environment, the artefacts of the built environment, and human biology, because we so often take them as the 'givens' of the situation being regulated. In many situations this is because they are non-malleable as constraints (rigid plasticity, in Lessig's terminology discussed below).

Lessig describes the equivalent of real space nature as "code, or the software that makes cyberspace as it is, ... a set of constraints on how one can behave". "The substance of these constraints vary, but they are all experienced as conditions on one's access to cyberspace".[38] His examples are whether or not passwords or other identification are required for access, whether encryption is allowed, and whether or not an individual's 'click stream' is tracked. He argues that is code/nature is more important in cyberspace regulation than in real space, for reasons explored in the following section.

D. Law: Direct and Indirect Regulation

Law typically regulates individual behaviour directly, and does so by threatening ex post facto sanctions. However, in real space as well as cyberspace, law also regulates individual behaviour indirectly, by aiming to change markets,

---

36 MA Lemley and D McGowan 'Legal Implications of Network Economic Effects' (1998) 86 *California Law Review* 479.

37 MA Lemley and D McGowan, *ibid* at 488-9.

38 L Lessig, note 29 *supra*.

norms or code. As others have done in different contexts, Lessig argues[39] that the anti-law Chicago School is misleading in that it assumes that the other constraints – markets, norms and code/architecture – are independent of law, but in fact they are in part a product of the law. We have to ask to what extent a particular constraint is created by law, and to what extent it can be changed by law. Law does not only affect individual behaviour directly (for example, by prohibiting certain conduct), but also indirectly by seeking to change markets, norms or architectures.

As in one of Lessig's examples,[40] governments can choose to address the barriers faced by disabled people by forbidding discriminatory conduct (direct regulation by law), by requiring educational institutions to teach children to respect the interests of the disabled (law indirectly regulating norms), or by requiring building codes to allow for access ramps and other physical facilities (law indirectly regulating real space 'code'). In real space, he argues, these indirect regulations are already 'the regulatory technique of choice'.

As will be illustrated later in this paper, law in cyberspace will often be more effective if it regulates code/architecture rather than trying to directly regulate individual behaviour.

V. FIVE FEATURES OF CYBERSPACE ARCHITECTURE AS REGULATION

There are some important general features of cyberspace code ('architecture' as I will call it), some of which are identified by Lessig.[41] They are explained here and illustrated in the examples that follow.

A. Architecture is More than Software

Lessig's characterisation of code as software ("code, or the software that makes cyberspace as it is") is an oversimplification. The equivalent of 'nature' in cyberspace needs to be understood as including a number of elements other than software, including at least hardware, Internet protocols and other standards, and aspects of human biology. Lessig is not consistent in limiting code to software, as he refers to "code ... or protocols", and includes in his examples of code both firmware (the 'V-chip') and a proposed protocol (PICS).[42] We need a more comprehensive statement of what is included in this constraint (and a better name).

Most obviously, we must include the hardware that comprises the physical infrastructure of cyberspace networks (such as routers, cabling, satellites). For example, although the Internet's protocols were designed to make particular physical connections irrelevant by allowing messages to route around outages, physical topography is still important in countries where governments only allow international connection to the Internet through a limited number of closely

39 *Ibid.*

40 *Ibid.*

41 L Lessig note 29 *supra*; points (ii), (iii) and (iv) in this section follow Lessig's approach, but (i) and (v) differ.

42 Platform for Internet Content Selection.

supervised junctions.

More important are Internet protocols (actual or proposed) such as TCP/IP, PICS, P3P or the Robot Exclusion Standard, not software in themselves but standards which can be implemented in software.[43] Protocols are code developed by participatory processes particular to the Internet, and are of vital importance as non-proprietary code.

Human biology can also be part of code, because various forms of biometrics will provide the 'authenticated' link between individuals and pervasive networks in the near future: identification is the 'real space/cyberspace interface'. Physical tokens (for example smart cards) are also important (at least for the time being), because they provide a portable link between individuals and networks.

If this argument is accepted, then 'code' becomes an inappropriate term, in that one of its usages is a synonym for software and thus is too narrow in its connotations. 'Code' is also far too ambiguous to be useful, since it is used in some contexts to refer to 'codes of conduct' (thus risking confusion with norms), and codification as opposed to less systematic laws (thus risking confusion with law). The term 'architecture' or 'cyberspace architecture' more fully expresses the nature of this constraint, and carries fewer ambiguous connotations. In my view 'architecture' should be used in preference to 'code'. In recent articles, Lessig has started to refer to "the architecture of privacy" and "the architecture of mandated access controls".[44]

The fact that cyberspace architecture has a number of components (software, protocols, hardware etc), is also helpful in explaining some differences in how these components operate as constraints. For example, in relation to the matters discussed below, protocols are usually less plastic than software.

B. Architecture has Immediacy as a Constraint

The directness or immediacy of a constraint ('A constraint is direct when its force gets applied immediately.') is one determinant of its effectiveness, the more direct the better. Real space architecture typically regulates more directly than law, which threatens punishment after the breach. It does not always enforce directly - 'the constraints of cancer are years away from the puff'.[45] The extent to which directness can be made to vary is a basis for choice between forms of regulation. Cyberspace architecture is often self-executing (for example, passwords and other forms of access controls), but not necessarily so.

C. Most Architecture has High Plasticity

The plasticity of a constraint is the ease with which it can be changed. Plasticity is a major variable in the extent to which law can regulate a constraint, with more plastic constraints more susceptible to change by law. The tides were not plastic at

---

43 R Clarke, G Dempsey, OC Nee and RF O'Connor 'A Primer on Internet Technology' available at <http://www.anu.edu.au/people/Roger.Clarke/II/IPrimer.html> provides brief explanations of Internet protocols and other standards.

44 See L Lessig, note 29 *supra* for article titles.

45 L Lessig, *ibid.*

all, as King Canute found. Australia's immigration constraints are premised on an absence of land borders with any other country, those of North American countries are not, and there is nothing any of them can do to change this. In other situations, the physical environment is a more plastic constraint. Architecture (in its real space sense) is very plastic while still in the planning stage (less so when built), and thus we have building codes. There is a great deal of choice in the nature and effectiveness of the constraints embodied in various styles of architecture, as Bentham stressed with his 'simple idea in architecture', the Panopticon.[46] In any given context where regulatory choice is being considered, the relative plasticity of the four types of regulation needs consideration.

Cyberspace architecture is inherently relatively plastic, since it is almost entirely a human artefact, whereas real space 'nature' is only partly artefact. This is one reason why law regulating cyberspace architecture is likely to be effective. It is generally possible for law to require changes to software, standards and hardware. Only a few aspects of cyberspace, such as those aspects of human biology with which it interacts, are impervious to law, and relatively few (perhaps some very basic protocols such as TCP/IP) would be very resistant to change by law.

D. The Legitimacy of Architecture Depends on Who Controls It

Recognition of the significance of cyberspace architecture as regulation forces us to look to its origins. Lessig poses the question:[47]

> Once it is plain that code can replace law, the pedigree of the codewriters becomes central. Code in essence becomes an alternative sovereign – since it is in essence an alternative structure of regulation. But who authors this sovereign authority? And with what legitimacy?

Control of cyberspace architecture is at present highly fragmented. Much of the most general architecture of cyberspace, protocols and standards, has been developed and is controlled by a variety of broadly representative and participatory non-government organisations of Internet governance, including the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), the Internet Society, the International Standards Organisation (ISO) and new players such as the gTLD-MoU. The fact that there is now far greater diversity of participants in global networks than when the Internet was a relatively homogenous and more technically-oriented community means that the consensus models of many institution of Internet governance will be under increasing strain, and subjected to increased demands to accommodate public policies,[48] as illustrated by the attempts to develop a new domain name system.

Governments already determine a considerable amount of the cyberspace architecture through legislation, as can be seen in the examples following. Increasingly, private companies such as Microsoft control significant parts of the

---

46 M Foucault, note 31 *supra* at 200-209.

47 L Lessig, note 29 *supra*.

48 Cf Reidenberg, note 25 *supra* at 592.

code of cyberspace through market share of a relatively small number of competing products such as browsers. As mentioned earlier, Boyle argues that digital libertarians have underestimated the extent to which both private power and governments already determine the architecture of cyberspace. Sometimes, the cumulative effect of individual users exercise significant control over architecture through market choices, as illustrated by the widespread usage of the PGP ('Pretty Good Privacy') encryption software. More often, intermediaries such as system operators or Internet Service Providers (ISPs) exercise significant controls over what is and is not possible by individual users.

In any given situation, one of the questions to be asked is whether an existing or proposed form of regulation by architecture is appropriate, given the nature of the regulator.

E. Default Settings Give Regulation by Default

The importance of the default settings in various forms of cyberspace architecture has not yet received sufficient emphasis. Architecture does not only make certain courses of action possible or impossible. It may theoretically leave open a number of possible courses of action in cyberspace, but one option will have the advantage of being set as a default. In real space, doors are lockable, but in houses the default setting is 'open', whereas in prison it may be 'locked'. The significance of default settings in cyberspace is illustrated in the examples following, particularly the example of cookies.

VI. REGULATION BY AND OF CYBERSPACE ARCHITECTURE: EXAMPLES

Having set out this sketch of a theoretical approach to regulation of cyberspace, the rest of this paper puts forward a number of examples which illustrate both differing aspects of how architecture regulates cyberspace, how cyberspace architecture is already regulated by law, and the regulatory choices that such an analysis can reveal. The work of Lessig, Boyle and Reidenberg provides extensive examples of architecture and its regulation in US law, often with a focus on content regulation and intellectual property. For non-American readers these examples are often complicated and made less relevant by legislative limits imposed by the US Constitution: the First Amendment is a local ordinance, after all. The examples following are drawn from universal Internet technical features, from Australian legislation, and from the German 'Multimedia Law',[49] one of the most extensive European attempts to regulate cyberspace architecture by law.

A. Building Anonymity into Architecture

The extent to which the surveillance capacity of cyberspace is limited, and

---

49 *Information and Communication Services Act* of 1997 (Informations- und Kommunikationsdienste-Gesetz - IuKDG) 1 August 1997- English translation at <http://www.iid.de/iukdg/iukdge.html>; see U Wuermeling, "Multimedia Law - Germany" (1998) 14 *Computer Law & Security Report* 41 for a summary; see also L Bygrave "Germany's Teleservices Data Protection Act" (1998) 5 *Privacy Law & Policy Reporter* 53.

where permitted made controllable by user choice, is perhaps the single key issue in the regulation of cyberspace.

Germany's *Teleservices Data Protection Act*[50] is a leading legislative example in addressing what the Germans call 'systemic data protection' ('Systemdatenschutz'), but we can also call 'legislating code'. The key provision requires the objective of minimising or eliminating the collection and use of personal information to be built into the 'design and selection of technical devices' (hardware and software) and thus into all aspects of cyberspace architecture:

> s3(4) The design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible.

It is this design requirement that makes the specific requirement on service providers to provide anonymous and pseudonymous uses of teleservices "to the extent technically feasible and reasonable"[51] a meaningful requirement, because it removes the excuse that systems have not been designed to allow for anonymous or pseudonymous transactions. Here, the control of code by law is both a serious, though general, limitation on the types of Internet systems that may be built, and a necessary precondition for legal sanctions aimed directly at the behaviour of service providers.

(i) The 'Anonymity Principle' in Australia

In Australia the 'anonymity principle' has been making progress toward becoming a legal requirement of cyberspace architecture. Its local origins lie in Principle 10 of the *Australian Privacy Charter* (1994): 'People should have the option of not identifying themselves when entering transactions'.[52]

In 1998 the Australian Privacy Commissioner's *National Principles for the Fair Handling of Personal Information*[53] included Principle 8 "Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions". The Victorian Government proposes to include a legislative formulation of these principles in its *Data Protection Act*.[54] One of the main differences between this formulation and that in the German law is that it does not have the explicit legislative requirement for systems to be designed to allow anonymity and pseudonymity, so it is possible that it may be interpreted to allow the excuse that it is not 'practicable' because the system design makes it technically impossible.

Somewhat more concrete requirements for code to allow anonymity may emerge from the Australian Commonwealth Government's development of standards for

---

50 Article 2 of the *Information and Communications Services Act* of 1997 - see references above.

51 s4(1) The provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed about these options.

52 Australian Privacy Charter Council (1994) *Australian Privacy Charter*, available at: <http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyCharter.html>, and explanatory material at <http://www.anu.edu.au/people/Roger.Clarke/DV/PrivChHist.html>.

53 <http://www.privacy.gov.au/news/p6_4_1.html>.

54 See G Greenleaf, "Will Stockdale Break the Privacy Impasse?" (1998) 5 *Privacy Law & Policy Reporter* 21 at 22.

the use of encryption technologies (both for digital signatures and confidentiality) in communications by and with Commonwealth Government agencies. The Government Public Key Authority (GPKA)[55] is considering requiring facilities for anonymity and pseudonymity to be designed in as a condition of accreditation of Certification Authorities (CAs) that wish to operate in the Commonwealth government sector, as part of the Government Public Key Infrastructure (GPKI).[56]

B. Cookies: Caller ID with Hidden Opt-Out

Cookies are an element of Internet protocols, server software and browser software which allow information to be placed on, and retrieved from, the user's hard disk during browsing of websites. Cookies allow a web server to 'know' such information as whether it has interacted with a particular user before, and to retrieve information from the user's hard disk about those previous interactions.[57] "Cookies are a way for a server to sustain a stateful session by passing information back to a user agent; the user agent returns the information back to the server on its next visit".[58]

Cookies are one of the most significant methods of surveillance of user browsing behaviour on the Internet. They provide a cost effective method of linking one instance of a user's browsing behaviour to another instance, allowing profiles of user behaviour to be created. They also allow the user's own hard disk to be used as a storage device for servers to record how they wish to interact with that user (for example, what type of advertisements to use).

Cookies were apparently an 'undocumented feature' in Netscape Navigator 2, with therefore no user control or knowledge as to when cookies were written or read during browsing. The existence and use of cookies prompted considerable protest by privacy organisations and others[59] from early 1996 onwards.

In Netscape Navigator Gold 3.0 (1996) the only options concerning cookies were (i) to accept all cookies without any warning (the default setting) or (ii) to be presented with an alert box every time before a cookie is accepted. There was no option allowing all cookies to be refused automatically without any alert box required.[60] The alert box is annoying, and responding to it slows down browser performance, so it is likely that many people would not change the default, even if they were aware it was possible to do so. Since the default was set at 'never

---

55 <http://www.gpka.gov.au/>.

56 Personal knowledge, due to the author's membership of the GPKA as a consumer representative. The GPKA has released 3rd Draft Criteria For Accreditation Of Certification Authorities (CAs)/Service Providers, but this element is not included in that draft: see <http://www.gpka.gov.au/working-groups/accreditation-evaluation/public/CAcriteria/CACriteria.htm>.

57 Netscape has described this as "Cookies are a general mechanism which server side connections (such as CGI scripts) can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent, client-side state significantly extends the capabilities of Web-based client/server applications." See quote at <http://www.epic.org/privacy/internet/cookies/>.

58 DM Kristol: <http://portal.research.bell-labs.com/~dmk/cookie.html>.

59 See 'The Coookies Page' (Electronic Privacy Information Center): <http://www.epic.org/privacy/internet/cookies/>.

60 This might mean that the browser could not access some pages, or even that occasional system crashes might result, but many users would prefer to have the option nevertheless.

warn', even the option to change would never be drawn to most users attention. In all these ways, the code conspired to maximise both the overt and covert 'acceptance' of cookies.

In Netscape Communicator 4.01 (1997), although the default setting is still 'Accept all cookies' (and do so without warning), it is now possible for users to choose to not accept cookies at all, or to only accept them after a warning. The result is that the code for cookies in version 4.01 is equivalent to caller-ID in telephony with the default set at opt-out (in secret, not drawn to the user's attention). Only the aware user can opt -out per line ('do not accept') or change the settings to the equivalents of per call opt-in ('warn me before accepting...'). It would be easy enough for the code to change the default setting to opt-in: the browser software would simply require the user to expressly opt in or out of accepting cookies, or (more drastic), change the default setting to 'do not accept'.

Also as Clarke points out,[61] the permission sought is only to write a cookie; cookies are automatically read by any servers who request them and know the ID of the desired cookie. There is a further option in Netscape Communicator 4.01 to accept only cookies that get sent back (only) to the originating server, at least allowing users to exclude cookies that can be read by servers run by third parties (which allows marketers to share user profile information).

Legislatures around the world have used law to regulate the consumer's options in relation to caller-ID. Regulation of the code of cookies presents similar policy choices. Germany's *Teleservices Data Protection Act*[62] deals with cookies in providing that 'in case of automatic processing' the user must be informed of the "type, scope, place and purposes" of collection of personal data "prior to the beginning of the procedure"[63] and also sets out ways by which consent can be given electronically. The overall effect on cookies would seem to be that browser code would have to be changed to accommodate one of the two opt-in approaches discussed above, but whether this has yet affected the operation of the Internet in Germany is not known.

C. Mandatory Surveillance Code: Interceptability and Decryption Ability

Surveillance of telecommunications by the state is an area where governments in Australia and elsewhere have shown little reluctance to legislate directly to require particular architectures for cyberspace. This is law mandating cyberspace architecture.

(i) Interceptability

Lessig gives the example of the 1994 US *Digital Telephony Act*[64] as a

---

61 R Clarke, "Cookies" (Version 1/6/98): <http://www.anu.edu.au/people/Roger.Clarke/II/Cookies.html>.

62 Article 2 of the *Information and Communications Services Act* of 1997 - see note 49 *supra*.

63 Section 3(5) provides in part "The user shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data. In case of automated processing, which permits subsequent identification of the user and which prepares the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure." Bygrave considers that the provision does affect cookies, note 49 *supra*.

64 PL NO 103-414.

requirement by Congress "that telephone companies select a network architecture that facilitates wire tapping".[65] In Australia the situation is much the same. The *Telecommunications Act* 1997 (Cth) Part 15 ('Cooperation with agencies') requires that carriers and carriage service providers must comply with obligations concerning interception capability and special assistance capability; must prepare and submit an annual interception capability plan; and must notify the Australian Communications Authority of technological changes affecting the provision of help to agencies in relation to carrying out of various law enforcement obligations under Part 14.[66]

These interception obligations are set by a determination by the Attorney-General, which "must specify an international standard or guidelines (the "international standard"), or the relevant part of the international standard, on which the determination is based" (s 322). The basis of this change resulting from the *Telecommunications Legislation Amendment Act* 1997 (Cth) is that:

> Australia has agreed to the use of International User Requirements at a meeting of the International Law Enforcement Telecommunications Seminar. This Bill will empower the Attorney-General to determine the specifics of interception capability. The capability requirements will be based on the International User Requirements[67]

This provision is therefore an example of cyberspace architecture in Australia being determined to a large degree by international agreements to which Australia is a party.

(ii) Decryption Ability

Although there is no direct prohibition on users sending encrypted messages over telecommunications networks, there are limitations on the extent to which carriers and carriage service providers can provide encryption services. Under the *Telecommunications Act* 1991 (Cth) licensing of network providers through the network service providers licences limited their ability to provide encryption facilities. The *Telecommunications Act* 1997 (Cth), as amended by the *Telecommunications Legislation Amendment Act* 1997 (Cth) also provides for 'special assistance capabilities' to be determined by the Attorney-General on the same basis as interception capability.

Keith Holland notes[68] that these requirements apply to both carriers and to carriage service providers, either of whom could be required "to include the ability to decrypt messages which may have been encrypted *by the carrier or service*

---

65 L Lessig, note 32 *supra*.

66 Summarising s 317 <http://www.austlii.edu.au au/legis/cth/consol_act/ta1997214/s317.html>.

67 Department of the Parliamentary Library <http://www.aph.gov.au/library/pubs/bd/1997-98/98bd067.htm>: Bills Digest No 67 1997-98 Telecommunications Legislation Amendment Bill 1997. See also N Waters, "Telecommunications interception - extending the reach or maintaining the status quo" (1998) 4 *Privacy Law & Policy Reporter* 110.

68 K Holland, Assistant Secretary, Security Law and Justice Branch, Attorney-General's Department, in "Recent International Legal Developments in Encryption" (IIR Conferences, 1998) available at: <http://www2.austlii.edu.au/itlaw/articles/Holland.html>. Holland seems to include decryption capacity as part of interception capacity, but the definition of 'interception' (s 320) means that it is more likely that decryption capacity is a 'special assistance capacity'.

provider as part of the normal operation of the service", but "does not, however, require carriers or service providers to decrypt traffic which has been encrypted by customers before being carried over the network". In summary, such restrictions do not prevent individual users from sending encrypted messages, but do limit the encryption services that carriers and service providers can provide. This is an example of law attempting to change cyberspace architecture by focussing on intermediaries (carriers and carriage service providers), while at the same time not attempting to regulate the equivalent activities of the end-users of telecommunications services because to do so would be futile.

D. Spam Black Holes: Is Law Safe for 'Return To Sender' Architecture?

The fight against unsolicited commercial email (commonly called 'spam') is an example of control of architecture, rather than law, being used to advance consumer and citizen interests rather than commercial interests. There are a variety of strategies and software being used,[69] of which the most extreme is the creation of spam 'black holes' such as that created by the MAPS (the Mail Abuse Protection System) RBL (Realtime Blackhole List)[70] which describes itself as:

> The MAPS RBL is a system for creating intentional network outages for the purpose of limiting the transport of known-to-be-unwanted mass email. The MAPS RBL is a subscription system, such that no one is ever denied connectivity to a non-RBL-subscriber. If your network seems to have been 'blackholed' by us, be aware that the places you cannot reach have deliberately chosen not to exchange traffic with you. We are not the network's police force, but rather, a method to identify likely spam origin.

Mail servers adopting the MAPS RBL refuse to exchange email with any mail servers listed in the MAPS RBL because they have been judged to be the sources of spam or relay spam email. Users of such mail servers find that much of the Internet treats them as a 'black hole' from which mail is not permitted to leave. This is cyberspace architecture which combines some technical features for transmission of information with a set of semi-formalised practices by those controlling email servers.

This is a consumer-controlled aspect of architecture that challenges law. The operators of MAPS RBL state that they have been often threatened with legal actions for conspiracy in restraint of trade[71] but none of the threatened actions has proceeded. This example shows the regulatory choices which are open: an alternative to legislation prohibiting spam is simply to ensure (if necessary) that restraint of trade laws do not impede operators of Internet black hole facilities. Such a choice, though some argue it is too weak a response,[72] would avoid making any individual conduct criminal or tortious (possibly ineffectively), and leaves the matter to code and the 'marketspace' of choices by mail server operators.

---

69 See CAUCE, The Coalition Against Unsolicited Commercial Email - <http://www.cauce.org/>.

70 See statement on MAPS RBL website at <http://maps.vix.com/rbl/>.

71 *Sherman Antitrust Act* actions in the USA.

72 See CAUCE, The Coalition Against Unsolicited Commercial Email - <http://www.cauce.org/>.

E. Platform For Privacy Preferences (P3P): What Can Protocols Achieve?

The World Wide Web Consortium (W3C) is developing the Platform For Privacy Preferences (P3P),[73] an Internet protocol which attempts to provide a framework to increase trust between web service providers and users of their services. As Roger Clarke explains,[74] the purpose of the P3P specification is to enable:

- websites to specify their personal data use and disclosure practices;
- web users to specify their expectations concerning personal data disclosure practices; and
- software agents to undertake negotiation, on behalf of the parties, in order to reach an agreement concerning the exchange of data between them.

In effect, it is to provide means whereby an individual can have sufficient information that he or she can make an informed decision on whether to permit further use of the data, or decline further use of the data. Moreover, that decision is to be able to be delegated to a software agent acting on behalf of the individual.[75]

P3P is a protocol which is intended to be able to be applied to support negotiations in a variety of Internet contexts, including explicit data provision (for example, answers to questions on web forms), implicit data provision (for example, capture of the 'click stream' or URLs of pages visited in succession), and explicit data provision from third sources (for example, a web user's stored profile of preferences, demographic details etc). How it can be applied to some extensions to basic HTML such as cookies and Java is not yet determined. P3P allows web users to have multiple digital pseudonyms (and therefore multiple digital personae), allowing a user to choose between a 'data-poor' or 'data rich' personality depending on the site visited.[76]

P3P is the first important privacy initiative to have emerged from the consultative and self-regulatory structures of Internet governance (although dominated by W3C staff members), and for that reason alone is of considerable significance. Otherwise, it is simply an example

Clarke compares what P3P is attempting to deliver against the OECD privacy Guidelines,[77] and concludes that it only addresses parts of three of the eight

---

73 See the Platform for Privacy Preferences pages on World Wide Web Consortium website at: <http://www.w3c.org/P3P/>.

74 R Clarke, "Platform for Privacy Preferences: An Overview", which is an excellent, simple overview of P3P: <http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html>.

75 *Ibid.*

76 Paragraph summarised from R Clarke, note 74 *supra.*

77 R Clarke 'Platform for Privacy Preferences: A Critique': <http://www.anu.edu.au/people/Roger.Clarke/DV/P3PCrit.html>.

OECD Principles.[78]

The more substantial criticism is that P3P says nothing about measures to ensure that it is complied with. If the web service provider breaches the practices that it has told the user that it adopts during a P3P 'negotiation' what can the user do about it (assuming he or she ever finds out in the first place)? P3P does not require the web service provider to log access and uses of the data it collects. P3P is not a certification scheme, and provides no guarantee of audits or similar protective measures (industry based certification initiatives like TRUSTe could supplement it). There is no guarantee that the P3P framework provides any linkage to a particular country's laws (such as contract laws or data protection laws), as Clarke points out, so P3P 'promises' may be legally meaningless. There is an 'assurance statement' in the Protocol where an attempt could be made to provide either contractually binding or legally descriptive statements, but its use is not compulsory.

P3P could develop as one of many useful forms of privacy protection, but it will be of little value unless it meshes with law and organisational practices. P3P is therefore an instance of where law is necessary to make protections offered by cyberspace architecture meaningful. Until law does that, P3P could be little more than a framework for deception.

The Electronic Privacy Information Center (EPIC) identifies a different danger: it considers P3P as, in effect, a framework for efficient collection of personal information as a condition of entry to websites. The possibility of increasing exclusion of those who value their privacy may make support for this initiative counter-productive to privacy, compared with simply opposing the increased collection of personal information.[79] EPIC's approach is one which would see limited value in law providing a legal framework to support and enforce P3P, and more value in legislation requiring architecture which supports anonymity, such as in the German law.

F. Stopping Searching - Robot Exclusion Standards

Internet-wide search engines such as Alta Vista and HotBot use robots (also known as spiders or webcrawlers)[80] to trawl the Internet, creating complete word occurrence indexes of every web page and every item posted to every News group that the spider is allowed to access.[81] As a result it is now possible to search for occurrences of a name or phrase occurring anywhere in the text of any web page, or in any News posting.

Web spiders and Internet search engines pose issues for copyright and privacy

78 It addresses data collection directly from the individual concerned, limitations on use and disclosure, and openness about use and disclosure policies, but does not address other principles relating to collection from third parties, subject access to data held by the web-site operator, retention of data and security. This is not necessarily a criticism, merely a limitation of one tool, but it would seem that some of these matters could be addressed by the same protocol in order to give more comprehensive privacy protection.

79 J Clausing 'Proposed privacy standards fail to please advocates of online privacy' 2 June 1998, *NYT Cybertimes* <http://www.nytimes.com/library/tech/98/06/cyber/articles/02privacy.html>.

80 See 'The Web Robots Page': <http://info.webcrawler.com/mak/projects/robots/robots.html>.

81 Many web robots are also self-limiting and only index sites down to a certain depth, so they are not comprehensive.

policies. It is possible that some Internet search engines might breach copyright laws (at least those which provide not just document titles in search results but short extracts as well), but in most cases the owners of such pages will welcome the extra access to their pages directed there by the search engine. Irrespective of copyright considerations some website operators might simply not want other search engines providing direct access to pages on their site, for reasons such as wanting users to use their own customised search engine instead, or because they do not think that web spiders update their indexes often enough, or because they are concerned that extensive access by robots will degrade performance of their server.

There is also a type of privacy issue. Technically, before robots can index any information on the web or in a newsgroup, it must have been made available to everyone on the Internet.[82] Nevertheless, many who place information on the Internet would not expect that it will be read by anyone outside those with whom they have some common experience, or the information used for purposes completely outside the intended purposes for which it was provided. For example, those involved in creating web pages, or involved in newsgroup discussions, concerning (say) gay and lesbian issues or issues relating to minority religious groups, could find that information about them was being systematically compiled and disseminated so as to harm them. Those who once valued the Internet as an escape from the values of small communities may find there is no longer any escape except behind barricades of secret communications.

Should there be some right not to be indexed? Legislative intervention would probably be dangerous, because this involves freedom of speech and freedom of the press considerations in a new context not just copyright and privacy. However, there are good reasons to accommodate the wishes of those who don't wish their pages to be indexed. Copyright law is likely to prove a very blunt instrument here. If, for example, copyright law was interpreted so that it was a breach of copyright to operate a web spider without obtaining the consent of each site indexed, the result would be that the cost of providing Internet-wide search facilities would rise very sharply, as operators of web spiders would be forced to obtain such consents in relation to millions of web pages. In all probability, only the few largest commercial players would have any prospect of sustaining such facilities, and far fewer pages would be indexed as operators would find it uneconomical to contact site owners who only provided a few pages. As a result the web could easily become unnavigable and impoverished as a source of information.

Can control of architecture provide an answer to this dilemma? There is a customary limitation on the operation of robots, which provides part of the answer. The *Robot Exclusion Protocol (1994)*[83] allows a server administrator to define[84] which parts of a website are not allowed to be indexed by robots (with exceptions for particular robots if desired). The default is assumed that if a site does not choose to exclude robots in this way, the whole of the site is available to

82 This must be done either by posting it to a newsgroup or putting it in a public_html directory or equivalent.

83 *A Standard for Robot Exclusion*: <http://info.webcrawler.com/mak/projects/robots/exclusion.html>.

84 In the file on the local URL "/robots.txt".

be indexed. The Protocol is not yet[85] any official Internet standard but rather "a common facility the majority of robot authors offer the WWW community to protect WWW server against unwanted accesses by their robots", and there are no sanctions against web spiders that ignore the Protocol and index sites or parts of sites contrary to instructions.

The authors of the Protocol recognised that it had limits because only a server administrator can maintain the list of pages on the server which are not to be indexed, not the owner of individual pages on the server. The Robots META tag has therefore been developed,[86] so that individual pages can contain information in their header that excludes robot indexing on a page-by-page basis. A tag of the form <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"> means that a robot should neither index this document, nor analyse it for links. The extent to which this tag is observed by robots (or used by page owners) is uncertain but seems not yet to be widespread, though its equivalent for Usenet posts is used widely.[87]

If there is near universal observance of the *Robot Exclusion Protocol* and the Robots META tag (when used) then this could be regarded as a reasonable resolution of the issue through a combination of architecture and self-regulation (norms or morality). Although it places the burden of opting out on those who do not wish their servers or pages to be searchable, this may well be a reasonable trade-off against the disastrous consequences for the Internet of requiring consent to be obtained from each individual page owner.

However, code and norms may not be enough. If the Protocol and the tag were ignored widely by robots, then legislation requiring the observance of such requests not to be indexed could be justifiable. This would be legislation requiring the observance of architecture which is not self-executing. On the other side of the coin, it might become necessary for legislation to provide a limited right to index, by ensuring that the transitory copying involved in the operation of a web spider was not prohibited, in which case legislation would be making architecture possible.

G. Electronic Copyright Management Systems (ECMS): 'IP Phone Home'

Digital libertarians expected intellectual property law to be one of the first casualties of cyberspace, because the process of digitisation of works made them infinitely reproducible at virtually no marginal costs, and infinitely distributable via the Internet. 'Everything [you know] about intellectual property is wrong'

85 There is now an 'Internet Draft', a working documents of the Internet Engineering Task Force (IETF), "A Method for Web Robots Control" (1996, expired June 1997): <http://info.webcrawler.com/mak/projects/robots/norobots-rfc.html>.

86 The Robots META tag is explained at: <http://info.webcrawler.com/mak/projects/robots/exclusion.html>#meta>.

87 Deja News, Alta Vista and some other search facilities allow users to insert the flag 'x-no-archive:yes' at the beginning of each post, and they are then not indexed. Old Internet information presents different problems. 'Living down' old Internet information is still possible. Web indexing engines only maintain details of current versions of pages. Some Usenet indexes such Alta Vista only retain postings for a few weeks or months, but DejaNews intends to archive all Usenet posts as far back as it can. However, it does accept requests for old posts to be deleted - again, an opt-out solution.

claimed John Perry Barlow.[88] As Lessig observes, infinite copies could only be made if "the code permits such copying", and why shouldn't the code be changed to make such copying impossible'?[89] It has only taken a few years for intellectual property to become one of the most controversial areas where cyberspace architecture is said to be replacing law as the most effective method of protection.

The controversy about electronic copyright management systems (ECMS), as copyright-protecting technologies are often called, stems from at least three main concerns:

- The architecture of ECMS need not observe any of the public interest limitations built in to copyright law . These include the right to lend a work for use by others (the basis of libraries, the 'first sale doctrine'), and the various 'fair dealing' rights to copy works or parts thereof for purposes such as 'criticism and review' or 'private study and research'. As Lessig puts it "what the law reserves as an limitation on the property holder's rights the code could ignore".[90] If dealings in relation to intellectual property become direct transactions where it is practical for the intellectual property owner to enter into a contract with the user (unlike the purchase of a book in a store), then such contracts are likely to routinely exclude such public interest exceptions.
- The enforcement of such contracts is also unlike real space contracts, Lessig points out, because whereas the law always takes into account various public and private interests in determining the extent and means by which contracts will be enforced, when contracts are self-enforced by code (for example, by the intellectual property suddenly becoming unusable) these public values are not likely to be taken into account.[91] We might add that when the law enforces a contract there is an independent assessment of whether there has been a breach of the contract, whereas here the enforcement is automated and unilateral, built into the architecture. If 'code contracts' replace law, these are not necessarily the same as 'law contracts', and may not be in the public interest.
- The amount of on-line surveillance of users of intellectual property may be unacceptable, compared with the ways in which we use intellectual property in real space, as discussed below.

There are numerous technologies and products now being developed which will provide different forms of technological protection to intellectual property: digital

---

88 JP Barlow, "Selling Wine Without Bottles: The Economy of Mind on the Global Net" *Wired* 2.03 (1993) at 86, available at: <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html>.

89 L Lessig, note 29 *supra* at "Code Replacing Law: Intellectual Property".

90 *Ibid.* Lessig also notes extensive argument in the USA as to whether "the fair use exceptions to copyright protection are not affirmative rights against the copyright holder, but instead the consequence of not being able to efficiently meter usage. Once that technical limitation is erased, then so to would the fair use rights be erased".

91 L Lessig, *ibid* at "Code Replacing Law: Contracts".

watermarks which include irremovable information about rights holders and/or licensees in the copyright work itself; search engines and web spiders routinely scanning the web for copies of identifiable digital works; on-line works that send reports back to a central location whenever they are used or copied ("IP phone home"); and cryptographic 'containers' which allow copies of works to be distributed widely but only used in full once a key has been obtained.

These are all important elements in the architecture that is being developed to protect intellectual property, but they are probably not the key element. What may make architecture replace law as the protection of digital intellectual property is a common framework for the trading of intellectual property rights, both between businesses and to end-users, a set of standards within which all of the particular IP-protective technologies can work.

(i) The Imprimatur Project: Europe's ECMS Code Development

In Europe the Imprimatur project,[92] sponsored by the European Commission, is developing such a model. The actors and inter-relationships in the Imprimatur Business Model, Version 2, are described briefly by Koelman and Bygrave:[93]

> In brief, the role of the creation provider (CP) is analogous to that of a publisher; ie he/she/it packages the original work into a marketable product. The role of the media distributor (MD) is that of a retailer; ie, he/she/it vends various kinds of rights with respect to usage of the product. The role of the unique number issuer (UNI) is analogous to the role of the issuer of ISBN codes; ie, it provides the CP with a unique number to insert in the product as microcode so that the product and its rights-holders can be subsequently identified for the purposes of royalty payments. The role of the IPR database provider is to store basic data on the legal status of the products marketed by the MD. These data concern the identity of each product and its current rights-holder. The main purpose of the database is to provide verification of a product's legal status to potential purchasers of a right with respect to usage of the product. As such, the IPR database is somewhat similar in content and function to a land title register. The role of the monitoring service provider (MSP) is to monitor, on behalf of creators/copyright-holders, what purchasers acquire from MDs. Finally, the certification authority (CA) is intended to assure any party to an ECMS operation of the authenticity of the other parties whom he/she/it deals. Thus, the CA fulfils the role of trusted third party (TTP).

From this brief description, some fundamental changes to the way in which copyright currently operates can be noted:

- Each digital artefact (including copyright works) is issued with a unique identification number,[94] which is then inserted by the content provided as microcode in the work to enable it to be tracked in various situations;
- There is an IPR database, 'somewhat similar in content and function to a land title registry', enabling anyone (particularly potential purchasers) to

92 Imprimatur: <http://www.imprimatur.alcs.co.uk/>.

93 K Koelman and L Bygrave, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems,* Institute for Information Law, (June 1998) p 5 (Report commissioned for the Imprimatur project): <http://www.imprimatur.alcs.co.uk/IMP_FTP/privreportdef.pdf>.

94 K Koelman and L Bygrave, note 93 *supra*, p 7.

verify a digital artefact's ID and legal status.

- There is a monitoring service provider (MSP) which, on behalf of creators and rights holders, will (though the summary does not say this) monitor transactions, uses and breaches (depending on the technology) of rights in digital artefacts. MSPs will use a variety of mechanisms, including reporting from Media Distributors, and surveillance of the web through the use of search engines, customised web spiders, and digital artefacts that report on their own usage.
- Certification Authorities (CAs) play a major role, as it assumed that both parties to transactions, and the authenticity of communications from them will be routinely identified by digital signatures, and so verification by CAs is needed.

This blueprint for the code in which intellectual property transactions will operate in cyberspace could hardly be more different than the real space code in which IP operates at present, and as regulation this code shares few similarities with IP law. This is not necessarily a criticism, merely an observation of how powerful and different code as regulation will be in intellectual property.

Koelman and Bygrave, while not opposed to ECMS, stress that the surveillance dangers are one of the most significant obstacles to the acceptable operation of ECMS:

> such systems could facilitate the monitoring of what people privately read, listen to, or view, in a manner that is both more fine-grained and automated than previously practised. This surveillance potential may not only weaken the privacy of information consumers but also function as a form for thought control, weighing down citizens with 'the subtle, imponderable pressures of the orthodox', and thereby inhibiting the expression of non-conformist opinions and preferences. In short, an ECMS could function as a kind of digital Panopticon. The attendant, long-term implications of this for the vitality of pluralist, democratic society are obvious.

(ii) The Propagate Project: An Australia's ECMS Development

In Australia the approach taken to ECMS by Imprimatur is being developed further by the Propagate project.[95] The model used by Propagate,[96] when fully developed, 'has the potential to become a standard in its own right and to be directly implemented in software'. Propagate is principally about the development of cyberspace code: at both the standards and software levels for digital

95 <http://www.propagate.net/> operated by Access CMC and Impart Corporation, and funded in part by DEETYA.

96 See <http://www.propagate.net/models.html>.

transactions.[97] The differences between the models being developed by Propagate and Imprimatur need not concern us here.

Propagate held its first Consensus Forum[98] in August 1998 with the aim of developing consensus within the Australian 'rights community' and others concerning both the accuracy and completeness of the model and the value of the ECMS approach.[99] Assuming that the model remains non-proprietary, Propagate's 'consensus' approach is obviously valuable in seeking input and consensus from 'stakeholders'. However, the consensus process seems relatively informal and closed, and is not yet a form of representative decision-making. For example, there was little explicit representation at the Forum of the users of copyright works, or of the broader public interests that copyright serves, though it was said that this will be remedied at subsequent meetings. This is simply an example of how, as Lessig put it 'once it is plain that code can replace law, the pedigree of the codewriters becomes central'. A framework for ECMS may become of the most important forms of architecture as regulation. Who controls and who participates in the development of this framework will be important, and might not be a matter on which consensus is easily reached.

H. Copyright Circumvention Devices: Protecting Architecture

The Australian Attorney-General has confirmed that

> The Government has decided to implement two new enforcement measures. One of the enforcement measures would ban commercial dealings in "black box" or other circumvention devices. There will also be a ban on the removal of copyright information electronically attached to copyright material."[100] (by which was meant 'rights management information').

These provisions will implement Article 11 and Article 12 of the WIPO *Copyright Treaty* 1996.[101] This is an early examples of international agreements being used to regulate cyberspace. Although they will affect use of technologies on CD-ROMs etc, their main effect will be in cyberspace. Both provisions will give legal support to the growing importance of architecture in the protection of

---

97 Propagate's objectives are stated to be: 'Propagate is a project to develop through industry, government and community based consensus a generally applicable conceptual model which describes a flexible system for the trading of intellectual property through the World Wide Web. The model will be propagated through stakeholders who participate in the evolution of the model. The Propagate Conceptual Model will be comprehensive, distributed, component based developed through a process of consensus with all the stakeholders, be they creators, agents, collecting societies, distributors, publishers or end users. It will be media, asset, and channel neutral to allow for flexibility, adaptability and growth. It may be deployed as a specification, discrete application or as an API to an existing application.' See: <http://www.propagate.net/project/objectives.html>.

98 The Consensus Forum details are at <http://www.propagate.net/consensus.html>.

99 Most of the copyright collecting societies and other major rights-holder organisations attended and were actively interested in ECMS development. The discussions at the Forum showed a lively sensitivity to privacy considerations, and recognition of the value of anonymous and pseudonymous transactions, but there were fewer ideas put forward on how to accommodate the 'fair dealing' issues discussed above.

100 Speech by Attorney-General Daryl Williams, "Copyright and the Internet: New Government reforms" para 35, 30 April 1998, Murdoch University - <http://law.gov.au/articles/copyright_internet.html>.

101 See Commonwealth Attorney-General's Discussion Paper *The Digital Agenda* "Part 5 - Proposed scheme for new technological measures and rights management information provisions" <http://law.gov.au/publications/digital.htm#anchor1565870>.

copyright through ECMS systems and other technological means. On the one hand they will make illegal any individual actions that will interfere with copyright management information which is part of the ECMS architecture. On the other hand they will make it illegal to deal in any way in 'black' architecture, hardware or software that could be used to circumvent copyright protections. Such provisions help make the Internet safe for ECMS.